Furman University
Electronic Journal of Undergraduate Mathematics
Volume **7, 1 − 11, 2001**

TILING BY (k, n)-CROSSES

JOANNE CHARLEBOIS

Abstract. We investigate lattice tilings of n-space by $(\mathbf{k}, \mathbf{n})$-crosses, establishing necessary and sufficient conditions for tilings with certain small values of k. We give a necessary condition for tilings corresponding to nonsingular splittings with general values of k. We also prove one case of a conjecture made by Stein and Szabó in [4].

1. Introduction

A (k, n)-cross is an n-dimensional object consisting of one central n-dimensional cube with an "arm" k cubes long attached to each of its $2n$ faces. See Figure 1 for an example.

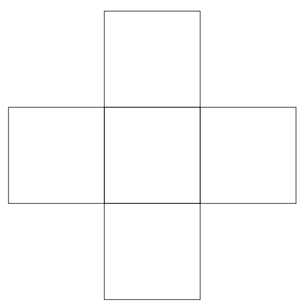

Figure 1. The (1, 2)-cross.

A lattice tiling of real n-space by (k, n)-crosses is a tiling in which each cube of a (k, n)-cross is centered on an integer lattice point, and each lattice point is covered by a cube from exactly one cross.

As shown in [4, p.62 and 75] the existence of a lattice tiling by (k, n)-crosses is equivalent to the following condition:

Condition 1. *Let $\mathbb{Z}_g$ denote the additive cyclic group of order g where $g = 2kn + 1$, and put $F(k) = \{\pm 1, \pm 2, \ldots, \pm k\}$. Then there exists a subset S of n elements of $\mathbb{Z}_g$ such that each nonzero element of $\mathbb{Z}_g$ can be written uniquely in the form fs with $f \in F(k), s \in S$, and 0 has no such factorization.*

Received by the editors January 5, 2001.
Key words and phrases. tiling, lattice tiling, splitting, cross, semicross.
This research was supported by NSERC Undergraduate Student Research Awards held in the summers of 1999 and 2000 under the supervision of Dr. J. D. Dixon. Thanks go to Scott Mutch for his computer programming expertise, and to Dr. Dixon for everything.

If Condition 1 holds then we call S a splitting set of $\mathbb{Z}_g$ by $F(k)$. A splitting is nonsingular if every prime divisor of g is $> k$, singular if any are $\leq k$, and purely singular if all prime divisors are $\leq k$.

It is known that a group G is split nonsingularly by a set M if and only if $\mathbb{Z}_p$ is split by M for each prime dividing the order of G ([4, p.71]).

In a singular splitting it is known the group looks like

$$G \simeq \mathbb{Z}_m \times \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \ldots \times \mathbb{Z}_{p_n},$$

for an integer m and primes p_i (not necessarily distinct), with $\mathbb{Z}_m$ split purely singularly and each $\mathbb{Z}_{p_i}$ split nonsingularly ([4, p.72 and 75]).

S. Szabó has proved that there are no lattice tilings by (k, n)-crosses when $k \geq n$ for $n > 1$ ([4, p.63]). Condition 1 makes it clear that the $(k, 1)$-cross for any k always tiles 1-dimensional space. (This is also true of the $(k, 1)$-semicross— see Section 5.)

As an illustration, consider $\mathbb{Z}_{17}$, corresponding to $2kn = 16$, so that $k = 2$ and $n = 4$. Then $F(2) = \{1, 2, 15, 16\}$, and the set

$$S = \{1, 3, 4, 5\}$$

is such that

$$F(2)S = \mathbb{Z}_{17} - \{0\}.$$

Thus the $(2, 4)$-cross lattice tiles 4-space. Note that S is not unique; other subsets of $\mathbb{Z}_{17} - \{0\}$ could also be taken as splitting sets.

Throughout this paper, k and n will be integers denoting the arm length of a cross and the dimension of space respectively, and p and q will always denote primes. Other lowercase letters will denote integers or residue classes of integers. As a splitting of $\mathbb{Z}_p$ is a factorization of $\mathbb{Z}_p^* = \mathbb{Z}_p - \{0\}$, we shall frequently identify the splitting with a factorization of $\mathbb{Z}_p^*$ in the obvious manner.

2. Tilings with small values of k

In this section we shall completely characterize the values of n for which there exist lattice tilings by (k, n)-crosses for some small values of k.

Lemma 1. *Consider any splitting of $\mathbb{Z}_p$ by a set F, with splitting set S. Then for all $m \not\equiv 0$, the intersection $mF \cap S$ has exactly one element.*

Proof. For all $s \in S$, $f \in F$ there is an m such that $s = mf$, since each f has a multiplicative inverse, and hence $s \in mF \cap S$. Thus

$$p - 1 \leq \sum_{m=1}^{p-1} |mF \cap S|.$$

If for the same value of m we have two pairs s, f and s_1, f_1 satisfying

$$s = mf \text{ and } s_1 = mf_1,$$

then $f_1 s = f_1 mf = fmf_1 = fs_1$. This is contrary to the uniqueness of the factorization into an element of F and an element of S. Thus $|mF \cap S| \leq 1$.

Therefore by the inequality above, $|mF \cap S| = 1$ for each m. □

Equivalently for $F = F(k)$,

$$|m\{1, 2, \ldots, k\} \cap \pm S| = 1 \text{ for all } m \not\equiv 0,$$

where $\pm S = S \cup \{-s : s \in S\}$, as this merely shifts the negative values from $F(k)$ into the splitting set. This is the form of the result we shall use most often.

Theorem 2. *The $(2,n)$-cross lattice tiles n-space if and only if the order $ord(4)$ of 4 in $\mathbb{Z}_p^*$ is even for each $p \mid 4n+1$.*

Proof. We know that the existence of a lattice tiling by the $(2,n)$-cross is equivalent to $\{\pm 1, \pm 2\}$ splitting $\mathbb{Z}_{4n+1}$, from Condition 1. Since $k=2$ and all $p \mid 4n+1$ are such that $p > 2$, any splitting of this group is nonsingular. Thus $\mathbb{Z}_{4n+1}$ is split if and only if $\mathbb{Z}_p^*$ factors for each $p \mid 4n+1$.

First let p be any prime dividing $4n+1$ and suppose $ord(4)$ is even, say $2m$, in $\mathbb{Z}_p^*$. We will show that this implies $F(k)$ splits $\mathbb{Z}_p^*$.

Since -1 is the unique element of order 2 in $\mathbb{Z}_p^*$, and 4 has even order, $-1 \in \langle 4 \rangle$. Thus $\langle 4 \rangle$ can be split by $\{\pm 1\}$, say

$$\langle 4 \rangle = \{1, -1\}T.$$

The factor group $\mathbb{Z}_p^*/\langle 4 \rangle$ has order ℓ where $\ell = (p-1)/2m$. If $2 \in \langle 4 \rangle$ then $2 = 4^i = 2^{2i}$ for some integer i. But then 2 (and hence 4) would have odd order which is contrary to our hypothesis. Thus $2 \notin \langle 4 \rangle$. Hence $2\langle 4 \rangle$ is an element of order 2 in $\mathbb{Z}_p^*/\langle 4 \rangle$ and so ℓ is even.

Therefore half the cosets are of the form $x\langle 4 \rangle$, the other half of the form $2x\langle 4 \rangle$ for a certain set of x's. Let U be a set of coset representatives for $\langle 2 \rangle$ in $\mathbb{Z}_p^*$ and note that $\langle 2 \rangle = \{1, 2\}\langle 4 \rangle$. Then

$$\begin{aligned} \mathbb{Z}_p^* &= \{1,2\}\langle 4 \rangle U \\ &= \{\pm 1, \pm 2\} T U \end{aligned}$$

is a factorization for $\mathbb{Z}_p^*$.

Now suppose S is a splitting set for $\mathbb{Z}_p$ by $F(2)$. We shall show that $ord(4)$ must be even.

We may assume $1 \in S$ ([4, p. 68]) which implies that $\pm 2 \notin \pm S$ due to Lemma 1.

Then, again from Lemma 1, $|2\{1,2\} \cap \pm S| = 1$ tells us that we must have $4 \in \pm S$. By induction on x, $4^x \in \pm S$ for all $x \geq 0$. Thus $\langle 4 \rangle \subseteq \pm S$.

Since $\pm 2 \notin \pm S$ from above, this shows that $\pm 2 \notin \langle 4 \rangle$.

Now $\mathbb{Z}_p^*$ is cyclic and so $\mathbb{Z}_p^*/\langle 4 \rangle$ is cyclic. Since $2\langle 4 \rangle$ and $-2\langle 4 \rangle$ both have order 2 in the factor group, they must be equal. Hence $2\langle 4 \rangle = -2\langle 4 \rangle$ and so $-1 \in \langle 4 \rangle$.

Therefore $|\langle 4 \rangle|$ is even, that is, $ord(4)$ is even.□

An equivalent formulation of Theorem 2 is that there is a splitting if and only if $\pm 2 \notin \langle 4 \rangle$ in $\mathbb{Z}_p^*$ for each $p \mid 4n+1$.

See Table 1 for the dimensions tiled by the $(2,n)$-cross with $n \leq 50$.

For $k=3$, there is also no possibility of singular splittings. If there was a singular splitting, the order of the group would be divisible by $p=2$ or $p=3$. These are both impossible since the order of the group is $6n+1$ for some n. Thus all splittings for $k=3$ are nonsingular, and we characterize them in the following theorem.

Theorem 3. *The $(3,n)$-cross lattice tiles n-space if and only if $\pm 2 \notin \langle 6, 8 \rangle$ in $\mathbb{Z}_p^*$ for each $p \mid 6n+1$.*

Proof. First note that $\pm 2 \notin \langle 6, 8 \rangle$ if and only if $\pm 3 \notin \langle 6, 8 \rangle$ since $6(\pm 3^{-1}) = \pm 2$ and $6(\pm 2^{-1}) = \pm 3$.

n	$2kn+1$
1	5
3	13
4	17
6	$25 = 5^2$
7	29
9	37
10	41
13	53
15	61
16	$65 = 5 \cdot 13$
21	$85 = 5 \cdot 17$
24	97
25	101
27	109
28	113
31	$125 = 5^3$
34	137
36	$145 = 5 \cdot 29$
37	149
39	157
42	$169 = 13^2$
43	173
45	181
46	$185 = 5 \cdot 37$
48	193
49	197

Table 1. The dimensions n lattice tiled by the $(2, n)$-cross for $n \leq 50$

We will now show that if there is a splitting, then $\langle 6, 8\rangle$ must be a subset of the splitting set $\pm S$, assuming $1 \in \pm S$.

As before, we may assume without loss of generality that $1 \in \pm S$. Suppose $r \in \pm S$. If $6r \notin \pm S$ then its factorization into an element of $\{1, 2, 3\}$ and an element of $\pm S$ is one of $6r = 2x$ or $6r = 3x$ for some $x \in \pm S$. Then we have $x = 3r$ or $x = 2r$ in $\pm S$, respectively, which contradicts $|r\{1, 2, 3\} \cap \pm S| = 1$ from Lemma 1. Thus we have $6r \in \pm S$.

We now know $r \in \pm S$ implies $6r \in \pm S$ and we know

$$|2r\{1, 2, 3\} \cap \pm S| = 1,$$

which implies that $4r \notin \pm S$. Thus if $8r \notin \pm S$ then we get $12r \in \pm S$ from

$$|\{4r, 8r, 12r\} \cap \pm S| = 1.$$

But, as we have $6r \in \pm S$, this contradicts

$$|\{6r, 12r, 18r\} \cap \pm S| = 1.$$

Therefore we must have $8r \in \pm S$.

Now for any $r \in \pm S$, we have $6r,\ 8r \in \pm S$, and we also have $1 \in \pm S$, which implies that

$$\langle 6, 8\rangle \subseteq \pm S.$$

Thus we need $\pm 2, \pm 3 \notin \langle 6, 8\rangle$ since otherwise this would contradict

$$|\{1, 2, 3\} \cap \pm S| = 1.$$

This proves the necessity of the theorem's statement.

To show that it is sufficient, note that the cosets of $\langle 6, 8\rangle$ partition $\mathbb{Z}_p^*$. Now we show that $x\langle 6, 8\rangle,\ 2x\langle 6, 8\rangle,\ 3x\langle 6, 8\rangle$ are distinct cosets for any x.

If there is a splitting, clearly

$$x\langle 6, 8\rangle \neq 2x\langle 6, 8\rangle \text{ and } x\langle 6, 8\rangle \neq 3x\langle 6, 8\rangle$$

as otherwise we would get 2 or $3 \in \langle 6, 8\rangle$, that is, 2 or $3 \in \pm S$. If $2x\langle 6, 8\rangle = 3x\langle 6, 8\rangle$ then $2\cdot 3^{-1} \in \langle 6, 8\rangle$, hence $6\cdot 2\cdot 3^{-1} = 4 \in \langle 6, 8\rangle$, which then gives $8\cdot 4^{-1} = 2 \in \langle 6, 8\rangle$, a contradiction. Thus the cosets as above are distinct.

Since $2 \notin \langle 6, 8\rangle$, the coset $2\langle 6, 8\rangle$ has order 3 in $\mathbb{Z}_p^*/\langle 6, 8\rangle$ and so

$$3 \mid [\,\mathbb{Z}_p^* \colon \langle 6, 8\rangle\,].$$

Therefore the number of distinct cosets must be a multiple of three. In fact the subgroup of $\mathbb{Z}_p^*/\langle 6, 8\rangle$ generated by $2\langle 6, 8\rangle$ is $\{\langle 6, 8\rangle, 2\langle 6, 8\rangle, 3\langle 6, 8\rangle\}$ since $2^2\langle 6, 8\rangle = 3\langle 6, 8\rangle$. Thus $\langle 2, 6, 8\rangle = \{1, 2, 3\}\langle 6, 8\rangle$. This means that the set of cosets can be factored by $\{1, 2, 3\}$, say

$$\mathbb{Z}_p^*/\langle 6, 8\rangle = \{1, 2, 3\}T$$

where T is a set of coset representatives for $\langle 2, 6, 8\rangle$ in $\mathbb{Z}_p^*$.

If $-1 \in \langle 6, 8\rangle$ then $\langle 6, 8\rangle$ is factored by $\{\pm 1\}$. Otherwise, $x\langle 6, 8\rangle$ and $-x\langle 6, 8\rangle$ are distinct for each x and so the set of all cosets can be factored by $\{\pm 1\}$. Either way as the cosets of $\langle 6, 8\rangle$ factor $\mathbb{Z}_p^*$ by $\{1, 2, 3\}$ we get

$$\mathbb{Z}_p^* = \{\pm 1\}\{1, 2, 3\}T_1 = F(3)T_1$$

as a factorization, where T_1 is a union of cosets of $\langle 6, 8\rangle$. $\square$

See Table 2 for the dimensions tiled by the $(3, n)$-cross with $n \leq 200$.

When $k = 4$, the only purely singular splitting is of $\mathbb{Z}_9$, as proved by Hickerson in [2]. Therefore we could have a mixed singular splitting for $k = 4$ of a group $G \simeq \mathbb{Z}_9 \times \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \ldots \times \mathbb{Z}_{p_n}$, in view of the result cited in Section 1.

Theorem 4. *The $(4, n)$-cross lattice tiles n-space if and only if:*
(1) $\pm 4 \notin \langle 6, 16\rangle$ in $\mathbb{Z}_p^*$ for each $p \mid 8n + 1,\ p \neq 3$;
(2) if $3 \mid 8n + 1$, then $9 \mid 8n + 1$ and $27 \nmid 8n + 1$.

Note that $\pm 4 \notin \langle 6, 16\rangle$ if and only if $\pm 2, \pm 3, \pm 4 \notin \langle 6, 16\rangle$.

The proof is omitted as it is similar to the proof of Theorem 3. The second condition for $p = 3$ takes into account a possible singular part to a splitting as $\mathbb{Z}_9$ can be split by $F(4)$.

See Table 3 for the dimensions tiled by the $(4, n)$-cross with $n \leq 500$.

For a purely singular splitting with $k = 5$, the order of the group would have prime factors $p = 2,\ p = 3$, or $p = 5$. We cannot have $p = 2$ or $p = 5$ as the order of the group is $10n + 1$ for some n. Thus the group has order 3^x for some x. Then all elements of the group that are relatively prime to 3 are those of the form

n	$2kn+1$
1	7
6	37
8	$49 = 7^2$
23	139
27	163
30	181
40	241
43	$259 = 7 \cdot 37$
52	313
56	337
57	$343 = 7^3$
58	349
63	379
68	409
70	421
90	541
95	571
101	607
105	631
125	751
143	859
146	877
153	919
156	937
162	$973 = 7 \cdot 139$
172	1033
181	1087
187	1123
190	$1141 = 7 \cdot 163$
195	1171

TABLE 2. The dimensions n lattice tiled by the $(3, n)$-cross for $n \leq 200$

n	$2kn+1$
1	9
12	97
109	$873 = 9 \cdot 97$
234	1873
270	2161
432	3457

TABLE 3. The dimensions n lattice tiled by the $(4, n)$-cross for $n \leq 500$

n	$2kn + 1$
1	11
12	$121 = 11^2$
42	421
70	701
133	$1331 = 11^3$
286	2861
393	3931
463	$4631 = 11 \cdot 421$

TABLE 4. The dimensions n lattice tiled by the $(5, n)$-cross for $n \leq 500$

$\pm fs,\ f \in \{1, 2, 4, 5\},\ s \in S,\ s$ relatively prime to 3. There are $\varphi(3x) = 2 \cdot 3^{x-1}$ such elements in the group. But

$$|\{1, 2, 4, 5\}| = 4 \not| \, 2 \cdot 3^{x-1}$$

so there cannot be such a splitting. Therefore all splittings for $k = 5$ are nonsingular, given by the conditions in the following theorem.

Theorem 5. *The $(5, n)$-cross lattice tiles n-space, for $n > 1$, if and only if $\pm 2, \pm 5, \pm 5 \cdot 2^{-1}, \pm 5 \cdot 3^{-1}, \pm 5 \cdot 4^{-1} \notin \langle 6, 32 \rangle$ in $\mathbb{Z}_p^*$ for each $p \mid 10n + 1$.*

Note that $\pm 2 \notin \langle 6, 32 \rangle$ if and only if $\pm 2, \pm 3, \pm 4 \notin \langle 6, 32 \rangle$.

The proof is omitted as it is also similar to the proof of Theorem 3. The extra conditions are necessary because otherwise the cosets

$$2\langle 6, 32 \rangle,\ 3\langle 6, 32 \rangle,\ 4\langle 6, 32 \rangle,\ 5\langle 6, 32 \rangle$$

may not all be distinct. For example, when $p = 101$ we have $10 \in \langle 6, 32 \rangle$ so that $3\langle 6, 32 \rangle = 5\langle 6, 32 \rangle$ and there is no splitting, although $\pm 2, \pm 3, \pm 4, \pm 5 \notin \langle 6, 32 \rangle$.

We require $n > 1$ in the theorem because when $n = 1$ we clearly have a splitting of $\mathbb{Z}_{11}$ by $F(k)$, but $\langle 6, 32 \rangle = \mathbb{Z}_{11}$.

See Table 4 for the dimensions tiled by the $(5, n)$-cross with $n \leq 500$.

3. A NECESSARY CONDITION FOR NONSINGULAR SPLITTINGS

We shall now give a necessary condition for a group of prime order p to be split by $F(k)$. As we show below, this condition is not sufficient, but it does appear to be a somewhat strong condition.

First, we introduce the notation for this section. Let g be a generator of the cyclic group $\mathbb{Z}_p^*$ and suppose that

$$F(k) = \{g^i\} \cup \{g^{i(p-1)/2}\}$$

with $i \in I$, where I is a subset of $\{1, 2, \ldots, p-1\}$. Define

$$a_0(x) = (1 + x^{(p-1)/2}),$$

$$a(x) = \sum_{i \in I} x^i,$$

and $f(x) = (x^{p-1} - 1)/(x - 1)$ in $\mathbb{Z}[x]$.

Lemma 6. *$F(k)$ splits $\mathbb{Z}_p^*$ if and only if there exist $b(x),\ c(x) \in \mathbb{Z}[x]$ such that $a_0(x)a(x)b(x) = f(x)c(x)$ where all nonzero coefficients of $b(x)$ equal 1 and $c(1) = 1$.*

Proof. Suppose there is a splitting $\mathbb{Z}_p^* = F(k)S$. Let $S = \{g^j : j \in J\}$ and define $b(x) = \sum_{j\in J} x^j$. For all $i \in I$ and $j \in J$ write

$$i + j = m(i,j) + n(i,j)(p-1)$$

with $0 \le m(i,j) < p-1$ and $n(i,j) = 0$ or 1.

Then the values of $m(i,j)$ run over the interval 0 to $p-2$, and so

$$a_0(x)a(x)b(x) = f(x) + (x^{p-1} - 1)\sum x^{m(i,j)}$$

where the sum is over all pairs (i,j) with $n(i,j) = 1$.

Thus $a_0(x)a(x)b(x) = f(x)c(x)$ where $c(x) = 1 + (x-1)\sum x^{m(i,j)}$.

Conversely, suppose

$$a_0(x)a(x)b(x) = f(x)c(x)$$

where $b(x)$ has the form $\sum_{j\in J} x^j$ for some subset J of $\{0, 1, \ldots, p-2\}$ and $c(x) \in \mathbb{Z}[x]$ has $c(1) = 1$. Then

$$c(x) = 1 + (x-1)c_0(x)$$

for some $c_0(x) \in \mathbb{Z}[x]$ and so

$$f(x)c(x) = f(x) + (x^{p-1} - 1)c_0(x).$$

Thus in the product $F(k)S$ each power $g^i,\ 0 \le i < p-1$, occurs an odd number of times, hence at least once.

Therefore, as $g^{p-1} = 1$, $a_0(x)a(x)b(x) = f(x)c(x)$ implies that $\mathbb{Z}_p^*$ factors in the form $\mathbb{Z}_p^* = F(k)\{g^j : j \in J\}$. $\square$

The next lemma uses information about the cyclotomic polynomials $\Phi_d(x)$ (see, for example, [1, Section 13.6]).

Lemma 7. *For $q^d \mid p-1$, the following are equivalent:*

(1) the cyclotomic polynomial $\Phi_{q^d}(x)$ divides $a(x)$;

(2) $a(g^h) = 0$ in $\mathbb{Z}_p^*$ for all g^h with h of the form $t(p-1)/q^d$, where $1 \le t \le q^d$ and $\gcd(t, q^d) = 1$.

Proof. Since $\Phi_{q^d}(x) = (x^{q^d} - 1)/(x^{q^{d-1}} - 1)$, the roots of $\Phi_{q^d}(x)$ in $\mathbb{Z}_p^*$ are just the elements ω such that $\omega^{q^d} = 1$ but $\omega^{q^{d-1}} \ne 1$ and hence are the primitive q^d-th roots of unity (these roots exist in $\mathbb{Z}_p^*$ since $q^d \mid p-1$). Thus $\Phi_{q^d}(x) \mid a(x)$ if and only if $a(\omega) = 0$ for each primitive q^d-th root ω of 1. The primitive q^d-th roots are of the form $\omega = g^h$, where $h = t(p-1)/q^d$, for t satisfying $1 \le t \le q^d$ and $\gcd(t, q^d) = 1$. $\square$

Theorem 8. *Suppose $\mathbb{Z}_p^*$ is split nonsingularly by $F(k)$, and let q be a prime dividing k. If q^e is the highest power of q dividing k, and q^{e_1} is the highest power of q dividing $p-1$, then for e values of d, with $1 \le d \le e_1$, we have*

$$\sum_{f\in F(k)} f^h \equiv 0$$

for each h of the form $t(p-1)/q^d$ where $1 \le t \le q^d$ and $\gcd(t, q^d) = 1$.

Proof. Over $\mathbb{Z}[x]$ the polynomial $f(x)$ is the product of the irreducible factors $\Phi_\ell(x)$, $\ell \mid p-1$, $\ell > 1$. Now $\Phi_\ell(1) = q$ if ℓ is a positive power of a prime q and $\Phi_\ell(1) = 1$ otherwise. Thus if $h(x)$ is a monic irreducible factor of $a_0(x)a(x)b(x) = f(x)c(x)$ and $h(1) \neq 1$, then $h(x) = \Phi_\ell(x)$ for some prime power $\ell > 1$. Since $a(1) = k$, this shows that for each prime $q \mid k$ there are exactly e values of $\ell > 1$, where ℓ is a power of q, such that $\Phi_\ell(x)$ divides $a(x)$ (where $1 < \ell \leq q^{e_1}$). Applying Lemmas 6 and 7 gives the result. □

Unfortunately the converse of this theorem does not hold. For example, take $p = 409, k = 4$. In this case we have

$$1 + 2^{(p-1)/4} + 3^{(p-1)/4} + 4^{(p-1)/4} \equiv 0 (\text{mod } p) \quad \text{and}$$

$$1 + 2^{(p-1)/8} + 3^{(p-1)/8} + 4^{(p-1)/8} \equiv 0 (\text{mod } p),$$

so that there are appropriate cyclotomic polynomials dividing $a(x)$ by Lemma 7. But we also have, in $\mathbb{Z}_p^*$, $16^{26} \equiv -4 (\text{mod } p)$, that is $-4 \in \langle 6, 16 \rangle$. As we have shown in Theorem 4, this means that there cannot be a splitting.

4. A conjecture of Stein and Szabó

In their book ([4, p.61]), S.K. Stein and S. Szabó state as an open problem the conjecture:

Stein/Szabó Conjecture:: If $n \geq 4$ and there is a lattice tiling by (k, n)-crosses then $k < n/2$.

It is easily shown that there are lattice tilings by (2, 4)-crosses and (3, 6)-crosses, but presumably these are the only exceptions where $k = n/2$.

As we shall explain below, this conjecture breaks up into two cases, and we settle the conjecture for one of the cases and give a necessary condition for the other case.

For the rest of this section, we assume that $2k \geq n$.

If we have a nonsingular splitting of $\mathbb{Z}_g$ where $g = 2kn + 1$ is not prime then there is a prime p dividing g with

$$p \leq \sqrt{g} \leq \sqrt{4k^2 + 1},$$

so $p \leq 2k - 1$ by hypothesis on n. A group G is split nonsingularly by $F(k)$ if and only if $\mathbb{Z}_p$ is split by $F(k)$ for each prime dividing the order of G, as noted in Section 1. But here the order of $\mathbb{Z}_p$ is at most $2k - 1$ so it cannot be split by $F(k)$ which has $2k$ elements. Thus if we have a nonsingular splitting of $\mathbb{Z}_g$, then $g = 2kn + 1$ must be prime.

Using Theorem 8, computations show that there are no nonsingular splittings of $\mathbb{Z}_{2kn+1}$ with $2kn+1$ prime and $2k \geq n$, for $4 \leq k \leq 200$; however we have not been able to settle the nonsingular case in general.

Theorem 8 implies that for prime k, because k does not divide n when $k > n/2$, a necessary condition for a splitting is that

$$\sum_{x=1}^{k} x^{2nt} \equiv 0 (\text{mod } p),$$

for $1 \leq t < k$ (where $p = 2kn + 1$). In terms of the Bernoulli polynomials $B_m(x)$, this requires

$$(1/(2nt + 1))[B_{2nt+1}(k + 1) - B_{2nt+1}(1)] \equiv 0 (\text{mod } p) \text{ ([3, p. 93])},$$

but we do not know of any results refuting the possibility of such a congruence. For composite k, there is more than one such congruence to check.

We now observe that if $\mathbb{Z}_g$ has a singular splitting, then this splitting is purely singular. Indeed, otherwise we would have a mixed singular splitting where $G \simeq \mathbb{Z}_m \times \mathbb{Z}_p$, with $\mathbb{Z}_m$ split purely singularly and $\mathbb{Z}_p$ split nonsingularly, from the results cited in Section 1. But, as we noted above the order of a group split by $F(k)$ must be divisible by $2k$, in this case $2k \mid m-1$ and $2k \mid p-1$, which leads to the contradiction $(2k)^2 \leq g = 2kn+1$. Thus any singular splitting of $\mathbb{Z}_g$ is purely singular, and so the problem is reduced to the nonsingular and the purely singular cases.

The following shows that the Stein/Szabó Conjecture is true in the purely singular case, that is, when each prime p dividing $2kn+1$ satisfies $p \leq k$.

Theorem 9. *If $k \geq n/2$ then there is no purely singular splitting of $\mathbb{Z}_{2kn+1}$ by $F(k)$.*

Proof. Fix a prime p dividing $g = 2kn+1$, and let s_p be the number of elements in the splitting set S with order divisible by the largest power of p dividing g. Write $k = p\lfloor k/p \rfloor + r_p$ where the remainder r_p satisfies $1 \leq r_p \leq p-1$ since p does not divide k.

Then

$$g - 1 = 2k(n - s_p) + 2ks_p$$

is the number of elements in $\mathbb{Z}_{2kn+1}$ with order greater than 1, and

$$g/p - 1 = 2k(n - s_p) + 2\lfloor k/p \rfloor s_p$$

is the number of elements with order greater than 1 but dividing g/p.

The two equations give:

$$\begin{array}{rcl} p-1 & = & -2k(n-s_p)(p-1) + 2s_p r_p \\ & < & -2k(n-s_p)(p-1) + 2(p-1)s_p\,, \\ \text{which yields} \quad s_p & \geq & (kn+1)/(k+1) \\ & > & n-2 \ \text{ since } \ n \leq 2k. \end{array}$$

Therefore we have $s_p \geq n-1$. If $s_p = n$ then

$$g/p - 1 = 2\lfloor k/p \rfloor n$$

from above and so $r_p = (p-1)/2n$. But, because $n > k > p-1$, $2n$ does not divide $p-1$ and so we conclude that $s_p \neq n$. Thus $s_p = n-1$. Moreover,

$$(p-1)(2k+1) = 2r_p(n-1).$$

This last equality shows that if $\gcd(2k+1, n-1) = 1$ then

$$2k+1 \mid r_p \quad \text{and so} \quad 2k+1 \leq r_p < p \leq k$$

which is not possible. Thus $\gcd(2k+1, n-1) > 1$. Let q be a prime such that q divides both $n-1$ and $2k+1$.

Then as $n \equiv 1 (\text{mod } q)$ and $2k \equiv (-1)(\text{mod } q)$, we get $g = 2kn+1 \equiv 0(\text{mod } q)$ and so we have $q \mid g$. Thus we can take $p = q$ in the above calculations.

Since $2k+1 \equiv 0(\text{mod } q)$, we have $k \equiv (q-1)/2(\text{mod } q)$, and hence

$$r_q = (q-1)/2.$$

$$\begin{aligned} \text{Then we have} \quad (q-1)(2k+1) &= 2(n-1)r_q \\ &= 2(n-1)(q-1)/2 \end{aligned}$$

which gives $2k + 1 = n - 1$, that is $n = 2k + 2$ contrary to $n \leq 2k$. This proves the theorem. □

5. Notes on semicrosses and on purely singular splittings

The set $S(k) = \{1, 2, \ldots, k\}$ corresponds to tilings by semicrosses, in which the k unit cubes extend out from only one side of the central cube. See Figure 2 for an example.

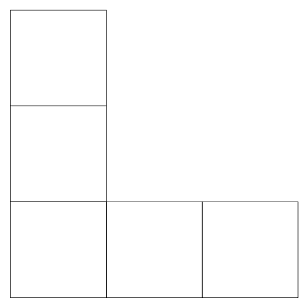

Figure 2. The (2, 2)-semicross.

It is known that a tiling by the (k, n)-cross implies a tiling by the $(k, 2n)$-semicross ([4, p. 63]). Thus the theorems in Section 2 give sufficient, but not necessary, conditions for lattice tilings by $(k, 2n)$-semicrosses with $k = 2,\ 3,\ 4,\ 5$. For example, when $k = 2$, if $ord(4)$ is even in each $\mathbb{Z}_p^*$ for all $p \mid 4n + 1$, then there is a tiling by the $(2, 2n)$-semicross.

Hickerson has shown (see [4, p.76]) that the only purely singular splittings by $S(k)$, for $k \leq 3000$, are of $\mathbb{Z}_{k+1}$ and $\mathbb{Z}_{2k+1}$ (corresponding to $n = 1$ and $n = 2$ respectively) when $k+1$ and $2k+1$ are composite. This implies that, for $k \leq 3000$, the only purely singular splittings by $F(k)$ are of $\mathbb{Z}_{2k+1}$ when $2k+1$ is composite. It is not known whether Hickerson's finding is true for general k. If it is, this implies that the only purely singular splittings by $F(k)$ are in dimension $n = 1$.

References

[1] D. S. Dummit and R. M. Foote, *Abstract Algebra*, Prentice-Hall, 1991.
[2] Dean Hickerson, *Splittings of finite abelian groups*, Pacific J. Math., **107** (1983), 141-171.
[3] K. S. Miller, *An Introduction to the Calculus of Finite Differences and Difference Equations*, Dover Publications Inc., 1966.
[4] S. K. Stein and S. Szabó, *Algebra and Tiling: Homomorphisms in the Service of Geometry*, The Mathematical Association of America, 1994.

Joanne Charlebois: Undergraduate at Carleton University, Ottawa, Ontario, Canada
E-mail address: ariix@inorbit.com

Sponsor: John D. Dixon, Carleton University, Ottawa, Ontario, Canada
E-mail address: jdixon@math.carleton.ca